

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BOARD OF PATENT APPEALS AND INTERFERENCES**

In re application of: Schwab et al.

Serial No.: 09/877,596

Group No.: 2157

Filed: June 8, 2001

Examiner: L. Jacobs

For: METHOD FOR SECURE TRANSACTIONS UTILIZING PHYSICALLY SEPARATED
COMPUTERS

APPELLANTS' CORRECTED APPEAL BRIEF

Mail Stop Appeal Brief
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the Notice of Non-Compliant Appeal Brief mailed April 7, 2008, Appellants' hereby submit their corrected Appeal Brief.

I. Real Party in Interest

The real parties in interest in this case are Barry H. Schwab and John G. Posa, individuals, Applicants and Appellants.

II. Related Appeals and Interferences

There are no appeals or interferences which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims

The present application was filed with 12 claims. Claims 1-12 are pending, rejected and under appeal. Claim 1 is the sole independent claim.

IV. Status of Amendments

No after-final amendments have been submitted.

V. Summary of Claimed Subject Matter

Independent claim 1 is directed to a secure transaction method (see Figure 1). The method comprises the steps of establishing an electronically accessible verification site authorized by the holder of a credit card (Specification, page 3, line 16 to page 4, line 3); receiving a request for goods or services at a merchant location using the credit card, but wherein the card is not physically presented to the merchant (Specification, page 2, lines 13-15); and accessing the verification site by the merchant to determine whether the request for goods or services is legitimate (Specification, page 4, lines 4-21).

VI. Grounds of Rejection To Be Reviewed On Appeal

A. The rejection of claims 1-4 and 7-12 under 35 U.S.C. §102(e) as being anticipated by U.S. Publ. No. 2001/0027527 to Khidekel et al.

B. The rejection of claims 5 and 6 under 35 U.S.C. §103(a) as being unpatentable over U.S. Publ. No. 2001/0027527 to Khidekel et al. in view of U.S. Publ. No. 2001/0051902.

VII. Arguments

Khidekel et al. is Not Prior Art

Despite the Examiner's objections, it is Appellants' contention that the instant invention was conceived of, and diligently reduced to practice, prior to the earliest priority date of the Khidekel et al. reference, namely, February 25, 2000. Both the inventors have submitted affidavits testifying to the fact that a disclosure document was transmitted from inventor Schwab¹ to inventor Posa² on February 20, 2000, five days earlier than the application date of the Khidekel et al. provisional application. Copies of the disclosure document and the affidavits of Messrs. Schwab and Posa are attached hereto for the Board's reference.

As the Board will see, the disclosure document is detailed, comprehensive, and directed to the

¹ Although the Examiner contends that Mr. Schwab failed to provide an affidavit, this is not the case (see attachments).

² Mr. Posa happens to be the patent attorney prosecuting this application.

claims of the instant application. The transmission of the disclosure document, namely, February 20, 2000, is not meant to identify the date of conception, but rather, is submitted to show that the inventors conceived of the invention *at least* five days prior to the provisional filing date of Khidekel et al. The Examiner argues at length that the inventors have “failed to show diligence,” but it appears to Appellants that the Examiner’s comments are simply boilerplate arguments copied from the MPEP, without regard to the facts of this case. Importantly, for example, the Board will note that the provisional application upon which the instant application relies was filed on June 9, 2000, slightly over two months after the transmission of the disclosure document. The Board will note that the provisional application adds further explanations regarding the basic disclosures made by the inventors, and both affidavits attest to the fact that various exchanges occurred during this time period, clearly representing diligence. As both affidavits are signed under oath, these should be taken as facts in support of the requisite evidence to establish diligence.

Based upon the statements and evidence of record, it is the opinion of Appellants that Khidekel et al. is not prior art, such that this case should be allowed.

Drawings

The objection to the drawings regarding the reference numeral 6 in Figure 1 was addressed in Applicant’s amendment to the first Office Action (September 3, 2004). Applicant amended the specification at page 3, line 20.

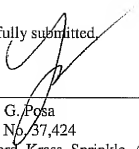
Conclusion

In conclusion, for the arguments of record and the reasons set forth above, all pending claims of the subject application continue to be in condition for allowance and Appellant seeks the Board’s concurrence at this time.

Respectfully submitted,

By: _____

Date: May 6, 2008


John G. Posa
Reg. No. 37,424
Gifford, Krass, Sprinkle, Anderson &
Citkowski, P.C.
PO Box 7021
Troy, MI 48007-7021
(734) 913-9300

APPENDIX A
CLAIMS ON APPEAL

1. A secure transaction method, comprising the steps of:
establishing an electronically accessible verification site authorized by the holder of a credit card;
receiving a request for goods or services at a merchant location using the credit card, but wherein the card is not physically presented to the merchant; and
accessing the verification site by the merchant to determine whether the request for goods or services is legitimate.
2. The method of claim 1, wherein the site is an electronic mail account.
3. The method of claim 2, wherein account was established by the merchant.
4. The method of claim 1, wherein an authorization message is sent from the site to the merchant in response to the step of accessing the verification site by the merchant.
5. The method of claim 4, wherein the authorization message is automatically generated.
6. The method of claim 4, wherein the authorization message is manually generated within a predetermined period of time.
7. The method of claim 4, wherein request for goods or services, the step of accessing the verification site, the authorization message, or any combination thereof, are encrypted.
8. The method of claim 7, wherein the encryption is implemented using an algorithm specific to the holder or an authorized user of the card.

9. The method of claim 4, wherein request for goods or services, the step of accessing the verification site, the authorization message, or any combination thereof, include routing information for future use.

10. The method of claim 1, wherein the step of accessing the verification site by the merchant causes an icon or window to appear in a web browser.

11. The method of claim 1, wherein the verification site is wirelessly accessible.

12. The method of claim 11, wherein the site is accessible through a cellular telephone, personal digital assistant, or other mobile device.

APPENDIX B

EVIDENCE

1. Affidavit of Barry H. Schwab
2. Affidavit of John G. Posa
3. Method for Secure Transactions Utilizing Physically Separated Computers

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Schwab et al.

Serial No.: 09/877,596

Group No.: 2157

COPY

Filed: June 8, 2001

Examiner: L. Jacobs

For: METHOD FOR SECURE TRANSACTIONS UTILIZING PHYSICALLY SEPARATED COMPUTERS

AFFIDAVIT OF BARRY H. SCHWAB
UNDER 37 CFR §1.131

I, Barry H. Schwab, make the following statements from my own personal knowledge under penalty of perjury:

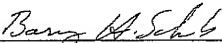
1. I am the first named inventor on U.S. patent application Serial No. 09/877,596 entitled "METHOD FOR SECURE TRANSACTIONS UTILIZING PHYSICALLY SEPARATED COMPUTERS." This application is based upon a provisional patent application filed June 9, 2000.

2. The claims of the subject application stand rejected, either under §102(e) or §103(a) over Khidekel et al., U.S. Patent Application Publication No. 2001-0027527A1. The '527 application is based upon a provisional application filed February 25, 2000.

3. I, together with my co-inventor John Posa, invented the subject matter disclosed and claimed in our pending application prior to the filing date of the Khidekel et al. application, such that this application should not be used as prior art.

4. Attached herewith is a document entitled "Method for Secure Transactions Utilizing Physically Separated Computers," which I forwarded to my co-inventor Mr. Posa on February 20, 2000, five days earlier than the earliest priority date to which Khidekel et al. are entitled. I conceived of the idea earlier than this, of course, and diligently reduced the invention in conjunction with my co-inventor through discussions and refinements which occurred on a regular basis up to the filing date of our provisional application.

FURTHER AFFIANT SAYETH NOT.


Barry H. Schwab

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

COPY

In re application of: Schwab et al.

Serial No.: 09/877,596

Group No.:

Filed: June 8, 2001

Examiner:

For: METHOD FOR SECURE TRANSACTIONS UTILIZING PHYSICALLY SEPARATED
COMPUTERS

AFFIDAVIT OF JOHN G. POSA
UNDER 37 CFR §1.131

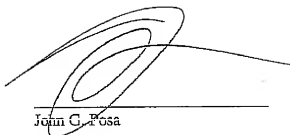
I, John G. Posa, make the following statements from my own personal knowledge under penalty of perjury:

1. I am a co-inventor named on U.S. patent application Serial No. 09/877,596 entitled "METHOD FOR SECURE TRANSACTIONS UTILIZING PHYSICALLY SEPARATED COMPUTERS." This application is based upon a provisional patent application filed June 9, 2000.
2. The claims of the subject application stand rejected, either under §102(e) or §103(a) over Khidekel et al., U.S. Patent Application Publication No. 2001-0027527A1. The '527 application is based upon a provisional application filed February 25, 2000.
3. I, together with my co-inventor Barry H. Schwab, invented the subject matter disclosed and claimed in our pending application prior to the filing date of the Khidekel et al. application, such that this application should not be used as prior art.
4. Of record in the prosecution file wrapper for our patent application is a document entitled "Method for Secure Transactions Utilizing Physically Separated Computers," which I received from my co-inventor Mr. Schwab on February 20, 2000, five days earlier than the earliest priority date to which Khidekel et al. are entitled.
5. Before and after the transmission of this document, Mr. Schwab and I diligently reduced the invention to practice through discussions and refinements which occurred on a regular basis up to the filing date of our provisional application.

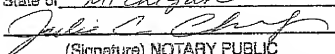
FURTHER AFFIANT SAYETH NOT.

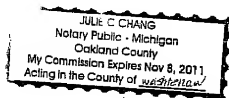
Serial No. _____
42904sh

- 2 -



John G. Posa

Subscribed and sworn before me, this 13th
day of September, 2005, a Notary Public
in and for Oakland County,
State of Michigan.

(Signature) NOTARY PUBLIC
My Commission Expires NOV 8, 2011.



Method for Secure Transactions Utilizing Physically Separated Computers

COPY

Field of the Invention

This invention relates to transactions conducted over computer networks, and, more particularly, to a system for securing transactions between physically separated participants from unauthorized users.

Background of the Invention

While the near-universal availability of the Internet to users in every location has created opportunities for many new kinds of businesses, it also has opened new opportunities for fraudulent use of credit card credentials by unscrupulous criminals. In these types of transactions (referred to as "card not present" transactions), the buyer of a product provides the seller with credit card information which cannot physically be verified, because the entire transaction occurs between remote participants and/or computers. Even in cases in which a customer service clerk speaks directly to the buyer to obtain the credit card information, there is no way to verify that the credit card credentials are legitimately obtained, or that the buyer is authorized to use the credentials to effect the transaction.

Various systems have been proposed or implemented in which the buyer is expected to provide information for verification, such as the maiden name of the buyer's mother, some form of biometric information, or a scan of the physical credit card through a remote reader in the buyer's computer. In each case, these types of data may be obtained through outside sources of information, simulated, or impersonated through computer means.

Summary of the Invention

In the instant invention, a method is disclosed by which verification of credentials may be accomplished using a separate, pre-established communications path. Whether the transaction is initiated by direct verbal contact or by computer communication over a wide-area communication network, such as the Internet, the credit card credentials are provided in the usual manner. After the credentials are recorded, the proposed transaction is forwarded to the credit card clearinghouse for authorization.

At this point, the credit card clearinghouse forwards a request for verification to an e-mail account which previously has been designated by the credit card holder. This could be an account maintained for the holder by the clearinghouse itself, or it could be an

independently maintained e-mail account at an "external" service provider. The request itself would carry sufficient information for the holder to identify the transaction items and the originating merchant; as an example, this would include information identifying the merchant, the items ordered, and the total amount requested to be approved. The holder then would be required to accept the transaction by acknowledging the contents of the e-mail message. If the user already is on-line with the merchant at the time of the transaction, it is a simple matter for the holder to open a new window in his or her "Browser" and retrieve this e-mail message. Current technology allows the use of various types of messaging "agents" which can provide near-immediate notification of the arrival of messages; another option would be to implement a wide-area communications protocol which would give priority to the carriage of certain types of transactional information and messages. In addition, software can be incorporated into the Browser application by which certain types of pre-configured communications links could be implemented with a single click of a computer "mouse".

For verbal orders, or in the case that the credit card holder cannot retrieve the e-mail message immediately, the holder would have a pre-determined period of time in which to perform the verification of the e-mail (for example, 12 hours) after which the transaction automatically would be canceled.

In an alternative embodiment, an "external" e-mail account could be programmed to automatically respond to a specific e-mail message by generating a reply message to be sent to the clearinghouse, similar to the manner in which e-mail systems automatically handle "spam" messages from identified senders. It also could respond by sending a message specific to the transaction that has been prepared in advance by the holder, in anticipation of the confirmation request from the clearinghouse.

A further enhancement would be to employ encryption to the various messages and responses, to ensure that only the credit card holder can access and respond to the messages. This encryption system could include the transmission and decoding of a specialized information file, which, among other things, could include information specific to the transaction (such as a transaction identifier or merchant number), or might require combination with additional information which would be provided by the holder. An alternative embodiment might include the application of an algorithm specific to the holder or to the transaction to modify existing data or to create new data as part of the verification method.

As an added benefit, the existence of routing information attached to the transmitted or returned messages would allow verification of the source computer for the response message, as well as providing an "audit trail" for the entire transaction.

APPENDIX C

RELATED PROCEEDINGS

None.